AMENDED IN SENATE JUNE 12, 2014

AMENDED IN ASSEMBLY MAY 23, 2014

CALIFORNIA LEGISLATURE—2013–14 REGULAR SESSION

ASSEMBLY BILL No. 2200

Introduced by Assembly Member John A. Pérez

February 20, 2014

An act to add and repeal Chapter 5.8 (commencing with Section 11549.50) of Part 1 of Division 3 of Title 2 of the Government Code, relating to cyber security.

LEGISLATIVE COUNSEL'S DIGEST

AB 2200, as amended, John A. Pérez. California Cyber Security Commission.

Existing law establishes various advisory boards and commissions in state government with specified duties and responsibilities. Existing law until January 1, 2015, establishes in state government the Department of Technology within the Government Operations supervised by the Director of Technology.

This bill would create the California Cyber Security Commission in the Department of Technology consisting of 12 members comprised of representatives from state government, appointed representatives from the private sectors in the technology or cybersecurity industry and utility, energy, or telecommunications industry, and an appointed representative of California's critical infrastructure interests. The bill would also authorize the commission to appoint representatives from state, local, federal, and private entities to form an advisory board in order to receive input or advice concerning the implementation of the duties of the commission. The duties of the commission would include establishing

cyber-attack response strategies and ~~defining a hierarchy of command within the state for this purpose~~ *performing risk assessments on state information technology systems.* The bill would require the commission to meet on a quarterly basis, or as specified, and would require the commission to issue a report on ~~a quarterly~~ *at least an annual* basis to the Governor's Office and the Legislature that details ~~the cyber security status and progress of the state and makes recommendations on how to improve the cyber security of the state~~ *the activities of the commission and makes recommendations to improve California's cybersecurity preparedness*.

The bill would abolish the commission, and repeal these provisions, on January 1, 2019.

Vote: majority. Appropriation: no. Fiscal committee: yes. State-mandated local program: no.

The people of the State of California do enact as follows:

SECTION 1. Chapter 5.8 (commencing with Section 11549.50) is added to Part 1 of Division 3 of Title 2 of the Government Code, to read:

CHAPTER 5.8. CALIFORNIA CYBER SECURITY COMMISSION

11549.50. The Legislature finds and declares all of the following:

(a) The State of California's growing dependence on technology has made it increasingly vulnerable to both foreign and domestic cyber security attacks. Thus far, there has been a fragmented approach to this issue with independent efforts occurring through federal, state, and local government, as well as in the state's universities and within private industry. For the purposes of public safety and protection of public assets, the state has a role in coordinating and improving its overall security and response capabilities.

(b) The market for cyber security is estimated to be more than seventy billion dollars ($70,000,000,000) in 2014. Of that amount, sixty-seven billion dollars ($67,000,000,000) is estimated to be spent nationally by private companies for computer and network security and the United States Department of Defense is planning to spend four billion six hundred million dollars ($4,600,000,000).

The United States Department of Defense is planning on spending twenty-three billion dollars ($23,000,000,000) over the next five years. Overall spending is expected to increase rapidly as recognition of threats becomes more ubiquitous. The California economy stands to greatly benefit from this industry growth.

(c) The State of California has already made investments for the purpose of cyber security; examples of which are research funding for the Lawrence Livermore National Laboratory and funding to augment a cyber security assessment and response team within the California National Guard.

(d) The California Cyber Security Task Force was initiated in May 2013 for the purposes of identifying critical threats, assembling primary stakeholders, and highlighting the growing importance of the issue. Among other things, this has increased awareness of the state's compliance with the new federal National Institute of Standards and Technology (NIST) standards and the Office of Emergency Services establishing Emergency Function 18, created particularly for cyber security.

(e) Over 50,000 new malicious online activities are identified every day, according to the United States Department of Defense. Incidents of sophisticated and well-coordinated attacks and data breaches are occurring more regularly, the average cost of which amounts to more than ten million dollars ($10,000,000). In 2012, a data breach to the state of South Carolina required more than twenty million dollars ($20,000,000) in response and restitution. The State of California is vulnerable technically, legally, and financially to these threats.

11549.51. (a) There is in the Department of Technology the California Cyber Security Commission. The commission shall consist of the following members:

(1) The Director of the Department of Technology, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the director's information technology and information security duties set forth in Chapter 5.6 (commencing with Section 11545).

(2) The Chief of the Office of Information Security, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the chief's information technology and information security duties set forth in Chapter 5.7 (commencing with Section 11549).

(3) The Director of Emergency Services, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the Office of Emergency Services's information technology and information security.

(4) The Attorney General, or his or her designee with knowledge, ~~expertises,~~ *expertise*, and decisionmaking authority with respect to the Department of Justice's information technology and information security.

(5) The Adjutant General of the Military Department, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the Military Department's information technology and information security.

(6) The Insurance Commissioner, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the Department of Insurance's information technology and information security.

(7) The Secretary of Health and Human Services, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the California Health and Human Services Agency's information technology and information security.

(8) The Director of Transportation, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the Department of Transportation's information technology and information security.

(9) The Controller, or his or her designee with knowledge, expertise, and decisionmaking authority with respect to the office of the Controller's information technology and information security.

(10) A representative from the private sector in the technology or cybersecurity industry, who shall be appointed by the Governor.

(11) A representative from the private sector in the utility, energy, or telecommunications industry, who shall be appointed by the Speaker of the Assembly.

(12) A representative of California's critical infrastructure interests, such as air traffic control, ports, and water systems, who shall be appointed by the Senate Committee on Rules.

(b) (1) Each representative appointed by the Governor, Speaker of the Assembly, or Senate Committee on Rules shall be appointed to serve a two-year term.

(2) Any representative may serve consecutive terms.

(c) Any designee shall serve at the pleasure of the official who designated them.

(d) Nine members shall constitute a quorum for the transaction of business, and all official acts of the commission shall require the affirmative vote of a majority of its members constituting a quorum.

(e) The members of the commission shall serve without compensation, except that each member of the commission shall be entitled to receive his or her actual necessary traveling expenses while on official business of the commission.

11549.52. (a) The commission may appoint representatives to form an advisory board in order to receive input or advice concerning the implementation of the duties of the commission.

(b) The advisory board may be comprised of one or more representatives from the following:

(1) The United States Department of Homeland Security.

(2) The National Institute for Standards and Technology.

(3) State government.

(4) Local government.

(5) California's utility grid, both private and public.

(6) Technology firms, cybersecurity firms, critical infrastructure operators, utility providers, financial firms, health care providers, and other private industries.

(7) California's cybersecurity law enforcement apparatus, which includes:

(A) The Attorney General's eCrimes Unit.

(B) The five regional task forces of the High Technology Theft Apprehension and Prosecution Program.

(C) The Department of the California Highway Patrol.

(8) Entities operating with the commission to perform its duties, including:

(A) The State Threat Assessment Center and fusion centers, for the purpose of sharing information that informs preventive actions.

(B) The California National Guard's Computer Network Defense Team, for the purpose of coordinating comprehensive risk assessments.

(C) California's public and private universities and laboratories for the purpose of directing research and best utilizing its results.

(c) The commission shall appoint each representative by a majority vote of its members constituting a quorum. Each representative shall serve at the pleasure of the commission.

11549.53. The commission shall meet quarterly, or more often as determined by a majority vote of its members constituting a quorum, or in the event of an emergency.

~~11549.54. (a) The commission shall focus on improving the state's cyber security and cyber response capabilities by developing partnerships with the public and private sector as well as the academic and nongovernmental world to share cyber security and cyber threat information to enable state government to protect and secure important information and data, intellectual property, financial networks, and critical infrastructure.~~

~~(b) The duties of the commission shall include, but not be limited to, the following:~~

~~(1) Working with the United States Department of Homeland Security to define a system of information sharing regarding cyber threat monitoring and response.~~

~~(2) Recommending minimum security standards for all state agencies.~~

~~(3) Researching in conjunction with academia and others to expand and improve state cyber security capability.~~

~~(4) Expanding public-private cyber security partnerships.~~

~~(5) Establishing cyber-attack response strategies and defining a hierarchy of command within the state for this purpose.~~

~~(6) Providing training for state employees and others to produce credentialed cyber security employees.~~

~~(7) Developing with the Department of Insurance a strategy to acquire cyber insurance for state agencies and assets.~~

~~(8) Proposing potential governmental reorganization to enhance the state's cyber security and response capabilities.~~

~~(9) Exploring fiscal options to fund the commission and its various activities, including the activities of some of its specific members, including the California National Guard's computer network defense team (CND).~~

~~(c) The commission shall issue a report on a quarterly basis to the Governor's Office and the Legislature that details the cyber security status and progress of the state and makes recommendations on how to improve the cyber security of the~~

~~state. The reports shall be submitted in compliance with Section 9795.~~

11549.54. The duties of the commission shall include the following:

(a) Developing within state government cyber prevention, defense, and response strategies and defining a hierarchy of command within the state for this purpose. This duty includes, but is not limited to, the following activities:

(1) Performing comprehensive risk assessments on state information technology systems. The Chief Information Security Officer shall coordinate the process of performing risk assessments and the assessments shall be performed by such entities as the California National Guard's Computer Defense Network Team and the State Threat Assessment Center, in addition to other public and private sector entities.

(2) Creating a risk profile of public assets, critical infrastructure, public networks, and private operations susceptible to cyber attacks.

(3) Coordinating efforts to reduce state information technology risks and gaps in existing service.

(b) Partnering with the United States Department of Homeland Security to develop an appropriate information sharing system that allows for a controlled and secure process to effectively disseminate cyber threat and response information and data to relevant private and public sector entities. This information sharing system shall reflect state priorities and target identified threat and capability gaps.

(c) Providing recommendations for information technology security standards for all state agencies using, among other things, protocols established by the National Institute for Standards and Technology and reflective of appropriate state priorities.

(d) Compiling and integrating, as appropriate, the research conducted by academic institutions, federal laboratories, and other cybersecurity experts into state operations and functions.

(e) Expanding the state's public-private cybersecurity partnership network both domestically and internationally to assist in the state's efforts to prevent and respond to cyber threats and cyber-attacks as well as enhance overall cyber detection capability.

(f) Developing and providing a training program to produce a credentialed and qualified state cybersecurity workforce. This

program should include training based in whole or in part on the requirements and protocols outlined in Department of Defense Directive 8570. The commission shall work with state workforce and labor entities as well as the state's higher education systems, federal agencies, and others to provide training and develop curriculum.

(g) Developing, in conjunction with the Department of Insurance, a strategy to acquire and incorporate cyber insurance into the procurement and administrative processes of state agencies to protect state assets and information.

(h) Expanding collaboration with the state's law enforcement apparatus assigned jurisdiction to prevent, deter, investigate, and prosecute cyber-attacks and information technology crime, including collaboration with entities like the High-Tech Theft Apprehension Program, and its five regional task forces, the Department of the California Highway Patrol, and the Attorney General's eCrimes unit. Collaboration will include information sharing that will enhance their capabilities including assistance to better align their activities with federal and local resources, provide additional resources, and extend their efforts into regions of the state not currently represented.

(i) Proposing, where appropriate, potential governmental reorganization options to enhance the state's cybersecurity assessment and response capabilities.

(j) Coordinating the pursuit of fiscal resources including federal grants and other funding opportunities to enhance the state's cybersecurity, information technology, data privacy, cyber research, and technology-based emergency response capabilities.

11549.55. The commission shall take all necessary steps to protect personal information, public and private sector data, as well as ensure consumer privacy, when implementing its duties.

11549.56. (a) The commission shall issue an annual report to the Governor's office and the Legislature, or more often if needed due to an emergency situation or time sensitive nature of a cyber event, that contains the following information:

(1) Details on the activities of the commission, including, but not limited to, progress on the commission's various tasks and actions taken and recommended in response to an incident, as appropriate.

(2) Policy, organizational, and investment recommendations to improve the cybersecurity preparedness of the state.

(b) The reports shall be submitted in compliance with Section 9795.

11549.57. This chapter shall become inoperative on January 1, 2019, and shall be repealed as of that date.

O